



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,092	10/03/2003	David Andrew Thomas	200309084-1	3543
<div>22879 7590 02/08/2008 HEWLETT PACKARD COMPANY P O BOX 272400, 3404 E. HARMONY ROAD INTELLECTUAL PROPERTY ADMINISTRATION FORT COLLINS, CO 80527-2400</div> <div>EXAMINER LANIER, BENJAMIN E</div> <div>ART UNIT PAPER NUMBER 2132</div> <div>NOTIFICATION DATE DELIVERY MODE 02/08/2008 ELECTRONIC</div>				

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No. 10/679,092	Applicant(s) THOMAS ET AL.	
	Examiner Benjamin E. Lanier	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 January 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) 18, 19, 24, 25 and 30 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17, 20-23, 26-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Election/Restrictions

1. Claims 18, 19, 24, 25, and 30 are withdrawn from further consideration pursuant to 37 CFR 1.142(b), as being drawn to a nonelected species, there being no allowable generic or linking claim. Applicant timely traversed the restriction (election) requirement in the reply filed on 04 January 2008.

2. Applicant's election with traverse of species 1 is acknowledged. The traversal is on the ground(s) that burden pursuant to MPEP section 808.02 has not been met. This is not found persuasive because the Examiner has provided rationale as to why the two species have separate status in the art.

The requirement is still deemed proper and is therefore made FINAL.

Specification

3. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The phrase "computer readable medium," is not found to have proper antecedent basis in the specification, however it is necessary to use this terminology in order to properly define the claim within the boundaries of statutory subject matter. In order to overcome the objection, an amendment to the specification is necessary constituting a non-exhaustive statement of what the phrase "computer readable medium" would be as it would have been known to one of ordinary skill in the art at the time of the invention, in order to verify that the term "computer readable medium," could not be taken in the context of non-statutory subject matter.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
 2. Ascertaining the differences between the prior art and the claims at issue.
 3. Resolving the level of ordinary skill in the pertinent art.
 4. Considering objective evidence present in the application indicating obviousness or nonobviousness.
5. Claims 1-17, 20-23, 26-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wisner, U.S. Patent No. 6,385,596, in view of Parenty, U.S. Publication No. 2002/0064283.
- Referring to claim 1, 3, 4, 20-23, 26-29, Wisner discloses an online music distribution system wherein a client transmits encrypted user information (i.e. credit card number), over the Internet using SSL v3, to a media licensing center enable purchasing of media content (Col. 13, lines 16-27 & Col. 16, lines 53-65), which meets the limitation of receiving from a device via an insecure communications channel at least one shared secret in encoded form that functions as an identifier of the device, the shared secret identifies a user, the shared secret is a credit card number. The user presents the content manager with a purchase voucher and if verified, the content manager sends the content key and encrypted content to the client (Col. 19, lines 15-38), which meets the limitation of transmitting encrypted content via the insecure communications channel from a

content server to the device, receiving a confirmation authorizing release of a decryption key, and sending the decryption key for decryption of the encrypted content, send the decryption key for decrypting the transmitted encrypted file for which the payment confirmation has been received, the confirmation is sent upon payment by a user of the device for the downloaded content. Wiser does not specify that the media licensing center/merchant server transmits the credit card information to the payment processor over a secure channel. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the elements of Figure 1B of Wiser to be connected using communications channels secured with physical protection measures in order to provide a means for communication sensitive information without having to utilize encryption techniques as taught by Parenty ([0033]). Figure 1B shows a content server, a point of sale terminal, and a payment server. Figure 1A shows one or more remote devices.

Referring to claim 2, Wiser discloses that the user presents the content manager with a purchase voucher and if verified, the content manager sends the content key and encrypted content to the client (Col. 19, lines 15-38), which meets the limitation of the confirmation is based on payment for the transmitted encrypted content.

Referring to claim 5, Wiser discloses that after transmission of the media content, which includes the media key, has completed, a notification is sent from the delivery system to the content manager (Col. 19, lines 44-49). Wiser does not disclose that the client sends a notification to the delivery system acknowledging completion of the media content download. However, Examiner takes OFFICIAL NOTICE that it is well known to those of ordinary skill in

the art at the time the invention was made that when a download has complete, a notification is sent to acknowledge the download completion.

Referring to claim 6, Wiser discloses that the encrypted media/media key is sent via the Internet (Figure 9BA, 960), which meets the limitation of the decryption key is sent to the device via the insecure communication channel.

Referring to claim 7, Wiser discloses that the media key is sent to the delivery system from the content manager (Figure 9BA, 954). Wiser does not specify that the content manager and the delivery system are connected via a secure channel. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the elements of Figure 1B of Wiser to be connected using communications channels secured with physical protection measures in order to provide a means for communication sensitive information without having to utilize encryption techniques as taught by Parenty ([0033]).

Referring to claim 8, Wiser discloses that the client transmits a randomly generated receipt to a delivery system (Figure 9BA, 948 & Col. 8, lines 32-34), which meets the limitation of receiving a random plaintext from the device.

Referring to claim 9, Wiser discloses utilization of SSL v3 (Col. 6, lines 15-23). Examiner takes OFFICIAL NOTICE that it is well known in the art that SSL v3 utilizes shared secrets encoded by a hash function of a combination of the shared secret and the random plain text as claimed.

Referring to claim 10, Wiser discloses that the content key is encrypted (Figure 9BA, 954), which meets the limitation of encrypting the decryption key before sending it to the device.

Referring to claim 11, Wiser discloses that the user presents the content manager with a purchase voucher and if verified, the content manager sends the content key and encrypted content to the client using SSL v3 (Col. 6, lines 15-23 & Col. 19, lines 15-38), which meets the limitation of the decryption key is encrypted using at least the shared secret, and optionally, the random plaintext secret because SSL v3 utilizes the shared secret and random numbers to generate keys used for encrypting/decrypting transmissions.

Referring to claims 12, 14, Wiser discloses that after transmission of the media content, which includes the media key, has completed, a notification is sent from the delivery system to the content manager (Col. 19, lines 44-49). Wiser does not disclose that the client sends a notification to the delivery system acknowledging completion of the media content download. However, Examiner takes OFFICIAL NOTICE that it is well known to those of ordinary skill in the art at the time the invention was made that when a download has complete, a notification is sent to acknowledge the download completion.

Referring to claims 13, 15, Wiser discloses utilization of SSL v3 (Col. 6, lines 15-23), therefore all transmissions would be protected using the SSL protocol which utilizes MD5 checksums for message authentication codes, which meets the limitation of the content download confirmation value is based on an MD5 checksum, receiving a random plaintext from the device, receiving a hash of the shared secret and the random plaintext for each shared secret, computing a hash of the shared secret with the random plaintext to produce a cyphertext for each shared secret, comparing the cyphertext to each of the received hash of each of the shared secrets, and in the case of a match, identifying the corresponding transmitted encoded content, encoding a content download confirmation value for the transmitted encoded content using the shared secret,

and comparing the computed content download confirmation value to the received content download confirmation value to verify a complete content download.

Referring to claim 16, Wiser discloses that the client can receive the content prior to purchasing (Col. 16, lines 4-40), which meets the limitation of after verification of the complete content download, causing a prompt to be sent to a user of the device to purchase the downloaded content, and receiving a confirmation of receipt of payment.

Referring to claim 17, Wiser discloses that the content is encrypted prior to being downloaded (Col. 19, lines 15-38), which meets the limitation of content stored in the content server is encrypted prior to a start of a download process.

Conclusion


6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 6:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Application/Control Number:
10/679,092
Art Unit: 2132

Page 8

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


Benjamin E. Lanier
Primary Examiner